APPENDIX A.1. GLOSSARY

Account fraud: There are two basic forms of account fraud – the misuse of a victim's existing account, and the opening of a new account in the victim's name. According to FTC research, about three-fourths of identity theft victims report that the thief misused only their existing accounts.[1] One-fourth of the victims report that the thief opened new accounts or committed other types of fraud with the victim's personal information. Credit card accounts are the most commonly misused *existing* account. Telephone accounts, usually wireless, are the most common type of *new* account opened by identity thieves. Identity thieves also open or raid bank accounts, Internet payment accounts, and auto, personal, or student loan accounts.

Blocking: Refers to a victim's right under §605B of the Fair Credit Reporting Act to prevent information that is the result of identity theft from appearing on her credit report.

Chronic Identity Theft: Also known as "revictimization." Occurs when a victim's identity is used more than once, often by different identity thieves, thereby forcing the victim to address repeatedly the identity theft-related problems.

Credit Report: (Sometimes called a "Consumer Report.") A communication of any information by a credit reporting agency that bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used to or expected to be used to establish a consumer's eligibility for credit, insurance, employment, or other purposes. Typically refers to the reports generated by Experian, Equifax, and TransUnion. But see "Specialty Consumer Reporting Agency."

Credit Reporting Agency: (Also known as a "CRA" Consumer Reporting Agency, and Credit Bureau.) A company that provides, assembles, and evaluates consumer credit information for the purpose of furnishing reports to third parties. Typically used to refer to Experian, Equifax, and TransUnion. But see "Specialty Consumer Reporting Agency."

Credit Freeze: A right provided by many states that allows identity theft victims and sometimes other consumers to block the access to the consumer's credit report by potential creditors, among others. The CRAs make this right available for a fee to consumers who reside in states that do not specifically provide the right to freeze.

Criminal Identity Theft: Criminal identity theft occurs when someone uses the victim's name and information as his own during an investigation, issuance of a ticket, or arrest by law enforcement. This may lead to the issuance of warrants or the entrance of guilty pleas in the victim's name. (For more information, see **Section IV.B**.)

Employment Identity Theft: Some identity thieves use a victim's Social Security number

[1] *Federal Trade Commission – 2006 Identity Theft Survey Report* (November 2007), available at http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

for employment. Identity thieves might use another person's identity if they have a criminal record that might prevent their being hired, or if they do not have legal status to work in this country. When this happens, the employer reports income earned by the thief to the Internal Revenue Service (IRS) and the Social Security Administration (SSA) using the victim's SSN, thereby creating income tax liability for the victim. (For more information on resolving identity theft-related questions with the IRS and the SSA, see **Section IV.D** and **E**.)

Equifax: Along with Experian and TransUnion, one of the three major nationwide credit reporting agencies.

Experian: Along with Equifax and TransUnion, one of the three major nationwide credit reporting agencies.

Fair Credit Billing Act: Also known as "FCBA." Federal law, codified at 15 U.S.C. §1601 *et seq.*, that provides rights and procedures that arise in relation to disputes regarding "open end" credit accounts, such as credit cards and revolving charge accounts.

Fair Credit Reporting Act: Also known as "FCRA." Federal law, codified at 15 U.S.C. §1681 *et seq.*, which establishes rights and duties with respect to credit reporting agencies.

Fair Debt Collection Practices Act: Also known as "FDCPA." Federal law, codified at 15 U.S.C. §§ 1692-1692p, which requires that debt collectors treat debtors fairly and prohibits certain methods of debt collection.

FCBA: See Fair Credit Billing Act.

FCRA: See Fair Credit Reporting Act.

FDCPA: See Fair Debt Collection Practices Act.

Federal Trade Commission: Federal government agency charged with enforcing various consumer protection laws and overseeing identity-theft related matters. Information on the FTC's identity theft programs can be found at www.ftc.gov/idtheft.

Furnisher: Also known as an "Information Furnisher." A creditor, debt collector, or other company that reports information about a consumer's credit payment history to a Credit Reporting Agency. For example, Joan Q. Consumer obtains a copy of her credit report from ABC Credit Bureau. The report shows that she was thirty days late in paying her XYZ credit card bill. ABC Credit Bureau is the credit reporting agency, and XYZ Credit Corp. is the furnisher of that payment information history

Fraud Alert: An alert placed on an identity theft victim's credit report to signal to creditors and other credit report users that the consumer has reported herself as a victim of fraud or at risk of identity theft. The creditor must take reasonable steps to confirm the

applicant's identity before issuing credit. Can be a 90-day alert or an extended alert that lasts for seven years.

Identity Theft Affidavit: A document designed to help victims establish their identity with creditors and substantiate their narrative of the fraud. Victims can use the FTC Identity Theft Affidavit to dispute accounts or transactions caused by the identity theft at the institutions where the fraudulent transactions occurred.

> Note: The Identity Theft Affidavit can be printed from the FTC's Website, either as a blank pdf form, or as a completed form. Victims who file a complaint online with the FTC can print the Affidavit filled with most of the information they entered. The Affidavit provides space to report multiple fraudulent accounts. When disputing fraudulent accounts or transactions with a particular company, the victim should consider providing to the company only information about the relevant accounts, possibly by redacting information about other accounts. Some companies require their own affidavit of identity theft forms.

Identity Theft Report: An official, valid law enforcement report that alleges the consumer's identity theft with specificity. It can be used to invoke certain statutory rights, including blocking identity theft-related information from appearing in the victim's credit report, preventing furnishers from continuing to furnish that information to any CRAs, preventing furnishers from selling or transferring the related debt for collection, and obtaining an extended fraud alert. An Identity Theft Report must contain sufficient detail for CRAs and information furnishers to verify the allegations of identity theft. To ensure that the Identity Theft Report contains sufficient detail, it is suggested that victims provide to law enforcement a completed Identity Theft Affidavit to attach to the police report. However, any police report containing sufficient detail can be an Identity Theft Report. For the purpose of obtaining an extended, seven-year fraud alert, which carries low risk of fraud, a completed Identity Theft Affidavit filed with the FTC and signed by the victim (but with no police involvement) provides sufficient detail. See **Section II.B** for more information about the Identity Theft Report.

Identity Theft Victims' Complaint and Affidavit Form: A form available on the FTC's Web site that is referred to elsewhere in this guide as the "Identity Theft Affidavit." Technically, it bears the full title, "Identity Theft Victims' Complaint and Affidavit" in recognition of its two functions: 1) when generated by the FTC's online complaint system, it is a record of the victim's complaint filed with the FTC; and, 2) it can be used as an Affidavit, *i.e.*, a voluntary statement of facts, sworn to by affirmation of the consumer signing it. The form, displaying most of the information provided in the victim's complaint, can be generated by completing the FTC Complaint Assistant, a guided interview process, or the blank form can be printed from the FTC Web site at http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf.

Medical Identity Theft: In cases of medical identity theft, thieves use a victim's name, and possibly insurance information to obtain medical services or goods. The victim is then saddled with proving she is not responsible for costly medical bills, or may find that the

thief has exhausted the victim's insurance coverage. Even worse, medical identity theft can have serious health consequences if the thief's real or fictitious medical information is added to the victim's medical records.

Mixed File: A credit file that has been corrupted by the inclusion of information associated with other individuals. In the case of an identity theft victim, a mixed file can result when the identity thief's application for credit provides a combination of the victim's information and someone else's information, such as using the victim's Social Security number and name, but providing his own or someone else's address, date of birth, or phone number. The victim's file can be corrupted when the creditor furnishes this mixed information to the CRA.

Mortgage Fraud: Identity thieves can steal a victim's identity in order to obtain a mortgage. In an emerging form of mortgage fraud, called "house stealing," thieves target an occupied home, assume the owner's identity, and have the home's deed transferred to the thief's name so that the victim no longer has ownership. NOTE: If you suspect house stealing, call the FBI immediately.

Revictimization: Also known as "chronic identity theft," occurs when a victim's identity is used more than once, often by different identity thieves, thereby forcing the victim to repeatedly address the identity theft.

Specialty Consumer Reporting Agency: (Sometimes known as a "Specialty CRA.") Company that creates consumer reports on consumer information other than credit, such as medical conditions, residential or tenant history and evictions, check writing history, employment background checks, and homeowner and auto insurance claims.

Synthetic Identity Theft: Each of the types of identity theft listed above involves the thief impersonating the victim to obtain benefits. In some cases the thief does not steal the victim's entire identity, but rather uses only the victim's Social Security number, in combination with another person's name and birth date, to create a new, fictitious identity. As a result, the victim may experience problems when the new identity tracks back to the victim's credit or tax records. Because this type of fraud may not be reflected on a consumer's credit report, it may not be discovered by the victim until many years later.

Tax Fraud: In this type of fraud, an identity thief files a tax return in the victim's name in order to receive a refund or other payment, such as a stimulus check. If the thief files for the refund before the victim, the IRS may deny the victim's rightful refund or stimulus check. (For more information, see **Section IV.D.**)

Trade Line: A section of a consumer report that provides information about an account such as when the account was opened and whether or not the consumer has made on-time payments on the account.

TransUnion: Along with Experian and Equifax, one of the three major nationwide consumer reporting agencies.